Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Service Rules for the 698-746, 747-762	)	WT Docket No. 06-150
And 777-792 MHz Bands	)	
	)	
Public Safety and Homeland Security	)	
Bureau Seeks Comment on Petitions	)	PS Docket No. 06-229
For Waiver To Deploy 700 MHz	)	
Public Safety Broadband Networks	)	
	)	
Amendment of Part 90 of the	)	WP Docket No. 07-100
Commission's Rules	)	
	)	

COMMENTS OF HARRIS CORPORATION

April 11, 2011

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Service Rules for the 698-746, 747-762	)	WT Docket No. 06-150
And 777-792 MHz Bands	)	
	)	
Public Safety and Homeland Security	)	
Bureau Seeks Comment on Petitions	)	PS Docket No. 06-229
For Waiver To Deploy 700 MHz	)	
Public Safety Broadband Networks	)	
	)	
Amendment of Part 90 of the	)	WP Docket No. 07-100
Commission's Rules	)	
	)	

To: The Commission

COMMENTS OF HARRIS CORPORATION

This Comment is submitted on behalf of Harris Corporation ("Harris") before the Federal Communications Commission ("Commission") in response to the Commission's *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*[1] ("*Fourth FNPRM*") seeking comment on a technical framework for ensuring the deployment and operation for a nationwide interoperable public safety network. Harris commends the Commission on its efforts to ensure that the highest level of interoperability is achieved across all forms of public safety communications. As the country approaches the ten-year anniversary of 9/11, we are all reminded of the life and death role that interoperable communications can play for first responders. The Commission has committed itself to creating an environment conducive to

[1] Service Rules for the 698-746, 747-762 and 777- 792 MHz Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, Amendment of Part 90 of the Commission's Rules, WT Docket No. 06-150, PS Docket No. 06-229, WP Docket No. 07-100, *Third Report and Order and Fourth FNPRM* (rel. Jan. 26, 2011) ("*Fourth FNPRM*").

interoperability. As the public safety communication solutions of tomorrow are deployed, the Commission is working to ensure that interoperability is considered at the outset and not as an afterthought. Harris is encouraged by the Commission's engagement on the operational, technical, and governance issues surrounding the deployment of broadband technology for public safety.

I. EXECUTIVE SUMMARY

While the Commission should continue to set an overarching regulatory framework for ensuring interoperability across the public safety broadband network, defining specific technical parameters and applications for the network should be left to the standardization process and designated standard setting organizations. Harris does not believe that every technical element of the public safety broadband network or applications riding on the network should be codified. The Commission must provide adequate flexibility to allow innovation to flourish and to enable optimization on a regional and/or jurisdictional basis. Codification of every technical element associated with the public safety broadband network will place public safety in a box and slow public safety's progression to the newest technology provided by the Long Term Evolution ("LTE") Standard. Network users must have the flexibility to work with standard setting organizations and vendors to implement capabilities beyond any minimum features adopted by the Commission—so long as they do not interfere with overall network interoperability.

In order to encourage interoperability across mission critical communications within a jurisdiction, Harris believes the Commission should continue to permit federal user access to the public safety broadband spectrum and determine that Section 337 permits network access to other non-federal entities that act in support of public safety's core mission (*i.e.,* to protect the safety of life, health or property). Allowing access by other entities that act in support of public

safety's core mission, such as critical infrastructure providers and transportation agencies, will offset build-out costs, leverage resources and increase interoperability. Providing non-public safety government and quasi-government organizations access to public safety broadband spectrum on a secondary basis, at the discretion of public safety, is permissible under Section 337. In order to ensure that the public safety broadband spectrum is being utilized in accordance with Section 337, the Commission can require permissible secondary users to enter into a "Sharing Agreement" with primary public safety "licensees." While the Sharing Agreements should be flexible to allow for different circumstances, the Commission can provide a draft sharing agreement containing certain guiding principles. The Sharing Agreement can then be filed with the Commission and Public Safety Broadband Licensee ("PSBL").

II. CORPORATE OVERVIEW

Harris is an international communications and information technology company serving government and commercial markets in more than 150 countries. Harris is a leading technology developer and manufacturer of mission critical wireless communications for the public safety communications market with more than 500 critical communications systems deployed world-wide. As a pioneer in the development of Internet Protocol ("IP") based networks for private radio and broadband applications, Harris supplies industry-leading brands such as VIDA Broadband™, P25^{IP}, EDACS®, OpenSky®, NetworkFirst™, and Provoice™. Harris is also an active member of numerous standards and technical committees including the Telecommunications Industry Association ("TIA"), the Emergency Response and Interoperability Center's ("ERIC") Public Safety Advisory Committee ("PSAC"), the National Public Safety Telecommunications Council ("NPSTC"), and Telecommunications Council, and the Alliance for Telecommunications Industry Solutions ("ATIS").

Harris is committed to providing public safety with solutions to achieving true nationwide interoperability through combining its leading Internet Protocol ("IP") based technology and in-depth knowledge of mission critical communications requirements. To meet the emerging needs of public safety for mobile broadband services Harris has developed VIDA Broadband LTE, a complete 700 MHz broadband network based on the 3GPP LTE cellular technology. VIDA Broadband LTE is a wireless broadband network designed exclusively for public safety, and uses the same fourth generation cellular network architecture and over-the-air technology, LTE, as commercial cellular networks. In addition, Harris now offers first responders full-spectrum multiband products for joint public safety operations on the local, state, and federal levels: the Harris Unity™ XG-100 and RF-1033M.

III. THE COMMISSION SHOULD CONTINUE TO PROVIDE GUIDANCE ON AN OVER ARCHING SET OF TECHNICAL PARAMETERS, BUT SHOULD LEAVE THE ADOPTION OF SPECIFIC TECHNICAL REQUIREMENTS TO THE STANDARDS PROCESS.

Harris believes that the Commission plays a vital role in providing a framework that ensures nationwide interoperability across the public safety broadband spectrum. There are two critical pieces in which the Commission must provide guidance in order to ensure that interoperability is achieved: (1) overarching technical parameters and (2) overarching governance structures. The current *Fourth FNPRM* primarily deals with the technical parameters of the public safety network. Harris commends the Commission on the activity in which it has engaged in to date to gather as much data as possible to ensure, from a technical standpoint, that interoperability is achieved across the public safety broadband network. However, Harris believes that not all technical requirements and capabilities should be codified. Specific technical details on network operation and applications should be left to designated standard setting organizations, such as ATIS. Harris also believes that the Commission's ERIC

will also play an important role in providing data and ensuring that as the network is rolled out, it is done in a matter that is consistent with the Commission's proposed definition of interoperability in the *Fourth FNPRM*.[2]

While discussed in-part within the *Fourth FNPRM*, Harris encourages the Commission to continue to advance discussion regarding network governance. To date, the Commission's efforts have been largely focused around the technical aspects of the proposed nationwide public safety broadband network. Determining how states should coordinate with individual public safety entities, local jurisdictions, the Commission, and the PSBL is vital to ensuring that the nationwide public safety broadband network meets the interoperability and operational needs of both the entire country and individual jurisdictions. Balancing the need for nationwide interoperability with the unique requirements and specifications of individual public safety entities is crucial to ensuring the real-world value of a nationwide public safety broadband network. Harris reiterates its request that the Commission issue a Public Notice (or even Notice of Proposed Rulemaking) on governance issues.[3] Such issues discussed in such a Commission item could include a licensing structure—both under current public safety broadband allocations and in anticipation of the reallocation of the D-Block—and the role of state governments in coordinating public safety broadband deployments. While a number of the questions related to governance were asked by the Commission in the *Second Further Notice of Proposed Rulemaking* and *Third Further Notice of Proposed Rulemaking* ("FNPRM"), some of those questions need to be re-explored in the context of the Commission's current network-of-

[2] "The Department of Homeland Security (DHS) Office of Interoperability and Compatibility (OIC), however, defines interoperability as "the ability of public safety agencies to talk to one another via radio communications systems – to exchange voice and/or data with one another on demand, in real time, when needed and when authorized." Id. at ¶ 16.

[3] Harris Corporation Request to Refresh the Record, PS Docket No. 06-229 (filed December 9, 2010) ("*Request to Refresh the Record*").

networks technical approach, current sentiment of the public safety community, and activity taking place in Congress regarding the D-Block.

A. Architectural Framework and Guiding Principles.

The Commission should define a single interoperability architecture to ensure interoperability across the nationwide public safety broadband network. Regardless of the amount of spectrum that is allocated to public safety for the deployment of the public safety broadband network—10 MHz or 20 MHz—the Commission must continue the process of establishing final governance and operational rules for the nationwide public safety network. Harris recommends that the Commission designate the states as the regional entities that have the role of coordinating 700 MHz broadband interoperability within their individual state and among states. This recommendation would ensure the Commission maintains a consistent policy on this issue. Specifically, Harris notes that the Commission has already designated interoperability channels in the 700 MHz and 800 MHz public safety narrowband spectrum. In the case of the 700 MHz narrowband interoperability channels, the Commission has granted administrative responsibility to the states, specifically either the State Interoperability Executive Committee ("SIEC") or an existing equivalent agency. In keeping with this established state-based framework, Harris recommends that similar administrative responsibility be granted to the states for the 700 MHz public safety broadband spectrum. Such a framework will also help more efficiently coordinate narrowband and broadband deployments to prevent interference.

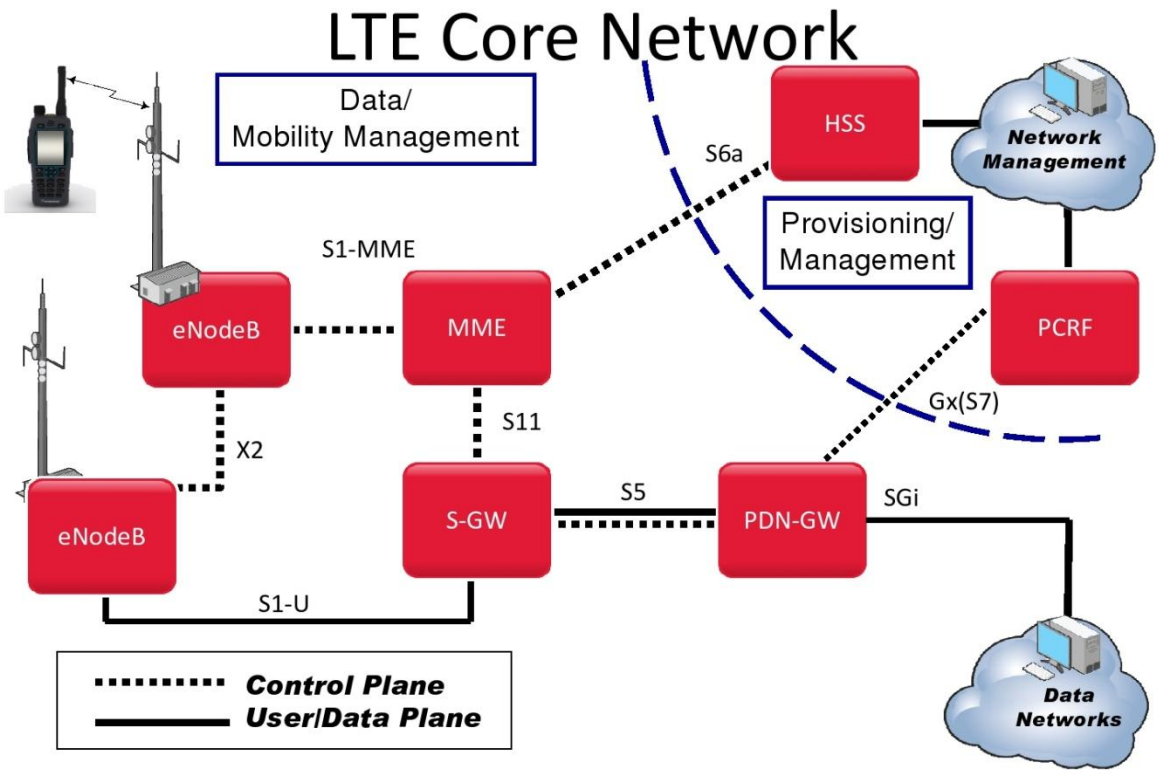
The Commission has expressed concern over the number of LTE "Cores" and subsequent Public Land Mobile Network ("PLMN") IDs, as a large number of disparate size Cores may overly complicate nationwide roaming. In order to alleviate concerns over an unmanageable number of PLMN IDs the Commission, through ERIC, should establish a regional governance

structure for the roaming portion of the LTE Core with a fixed number of PLMN ID's. It is Harris' view that the logical regional governance entity for this "regional Core" should be each individual state. In addition, the Commission should encourage the build-out of 700 MHz radio access networks ("RAN") by allowing for regional entities to utilize distributed data transport Core(s) that may be connected to the regional interoperability Core for the purpose of nationwide roaming.

Harris believes that the Commission should not dictate specific system architectures for each local, state or regional network and should allow for flexibility in the build-out of local networks. However, Harris believes that the Commission should define a single interoperability architecture, at the state level. Each state should be responsible for ensuring that local or regional networks built-out within that state satisfy the uniform statewide interoperability architecture. Therefore, it would be appropriate for the Commission to require that waiver grantees receiving a certification under the geographic coordination process commit to complying with the future state interoperability architecture and demonstrate in their Interoperability Showing how compliance will occur.

In general, the evolved packet Core ("EPC") of the LTE network is considered as a single entity and is often referred to as the "Core." The Commission is right to be concerned about the number of Cores that may proliferate in a nationwide network, and the method for managing interoperability in a nationwide network built from these Cores. However, the LTE EPC is actually constructed from two logical entities, which for the purposes of discussion, may be referred to as the "Provisioning/Management Core" and the "Data Transport/Mobility Management Core," as illustrated in Figure 1.

Figure 1

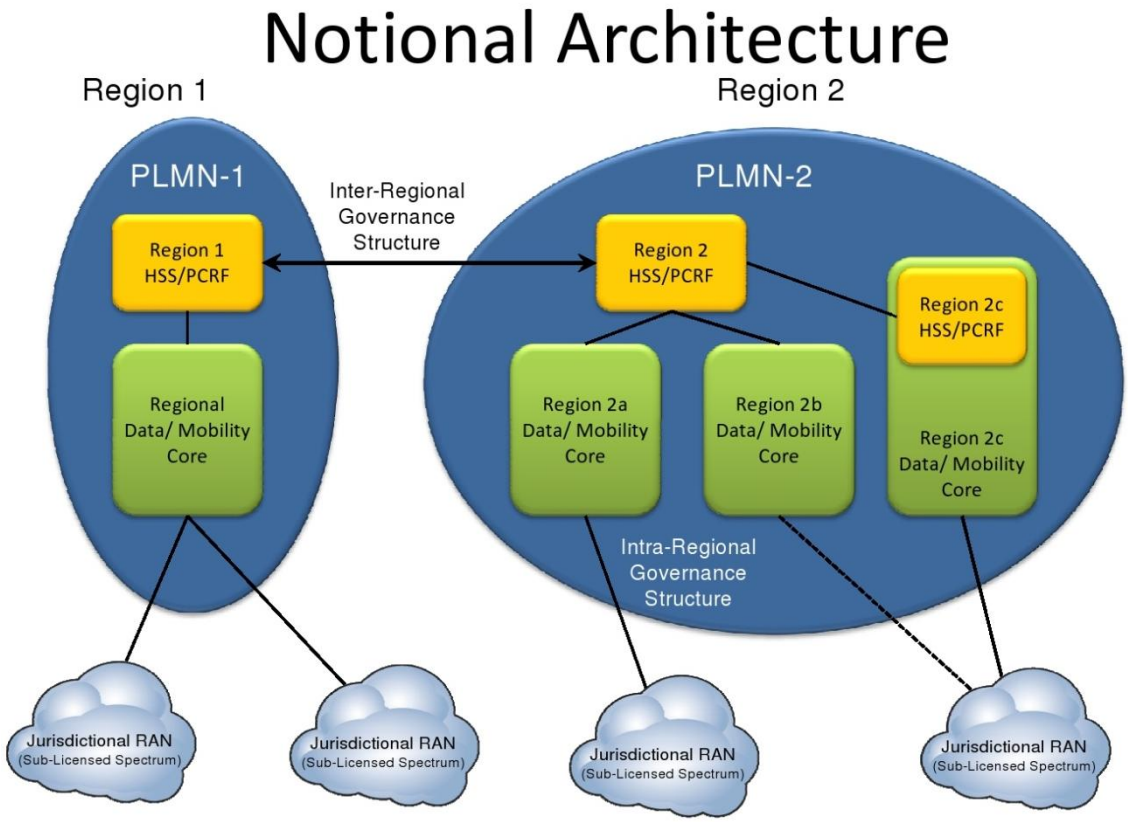


The local Data Transport Core includes the MME, S-GW, and PDN-GW elements. Due to the substantial backhaul requirements of LTE (50Mbps – 100Mbps per site), it is generally desirable that these entities be close to the RAN. The Provisioning Core consists of the HSS and PCRF elements. This Core contains user profiles and authentication information for all users in a region. As this is a centralized function for the network, it is logical that this entity be centralized. Further, the centralization of this function provides a central entity that supplies the roaming anchor for transfer of user authentication and provisioning data for roaming users. The management of the provisioning Core requires substantial governance resources, as the governing entity must manage all user configuration information as well as roaming addresses/agreements between adjacent regions. For this reason, Harris recommends that the appropriate governance structure should take place on the state level.

In practice, each region will require a single centralized HSS provisioning Core and each Core will be assigned a unique PLMN ID. The other Core network elements may be distributed throughout the transport network. A region may choose to have distributed local HSS for sub-region traffic, but it must "roll up" to a centralized HSS. Some regions may choose to have a single centralized Core for the whole network. Other regions may choose to subdivide the network below the centralized HSS to allow for regionally distributed sub-Cores. Harris believes that allowing for flexibility within the framework of a nationwide roaming architecture will promote broadband deployments that meet the unique needs and requirements of public safety entities, while maintaining the Commission's goal of ensuring nationwide interoperability.

By allowing for a flexible distributed network within a large state, the Commission will allow for a more robust architecture that meets local needs. The following diagram, labeled as Figure 2, illustrates the Notional Regional Architecture where each region has a centralized provisioning Core, but may choose to have regional flexibility below that structure. For example, if for some reason region 2b in Figure 2 loses connection to the State Interoperability HSS due to a large scale catastrophic event, the local region will have the ability to continue to operate their local network during this emergency. This level of flexibility and redundancy may be very important to certain regional entities. Harris recommends that the Commission consider this regional architecture, with a centralized regional roaming entity, as a model for the nationwide public safety broadband network's regional architecture.

Figure 2



B. System Identifiers.

Harris supports the proposed hybrid scheme of one separate PLMN ID assigned to each tribal or regional network and a single overall PLMN ID assigned for the overall network.[4] This approach offers the following advantages:

- Regional administrators are able to maintain control over the administration of their regional network.
- Users home HSS can be identified by the PLMN ID portion of their IMSI.
- Roaming users can use the nationwide PLMN ID.
- Roaming profiles can be defined nationally for users within the national PLMN ID.
- Federal and other non-regionally homed users can access the network using the nationwide PLMN ID.

[4] Fourth FNPRM, *supra* note 2, at ¶ 33.

As stated above, Harris recommends the use of regional PLMN ID's along with a nationwide PLMN ID for roaming. That said, the regional architecture advocated by Harris can be implemented through the use of the single nationwide PLMN ID. In this case of a single PLMN ID, the available IMSI domain would need to be portioned among the regional networks and Diameter Proxy or Redirect Agents would need to be deployed so MMEs could find the Home HSS of roaming users.

Harris believes that regional Cores should be defined at the state level. However, to provide for local flexibility each regional Core could contain sub-regional Cores. Figure 3 below lays out the proposed regional network architecture and Figure 4 illustrates the sub regional Core architecture.

Figure 3

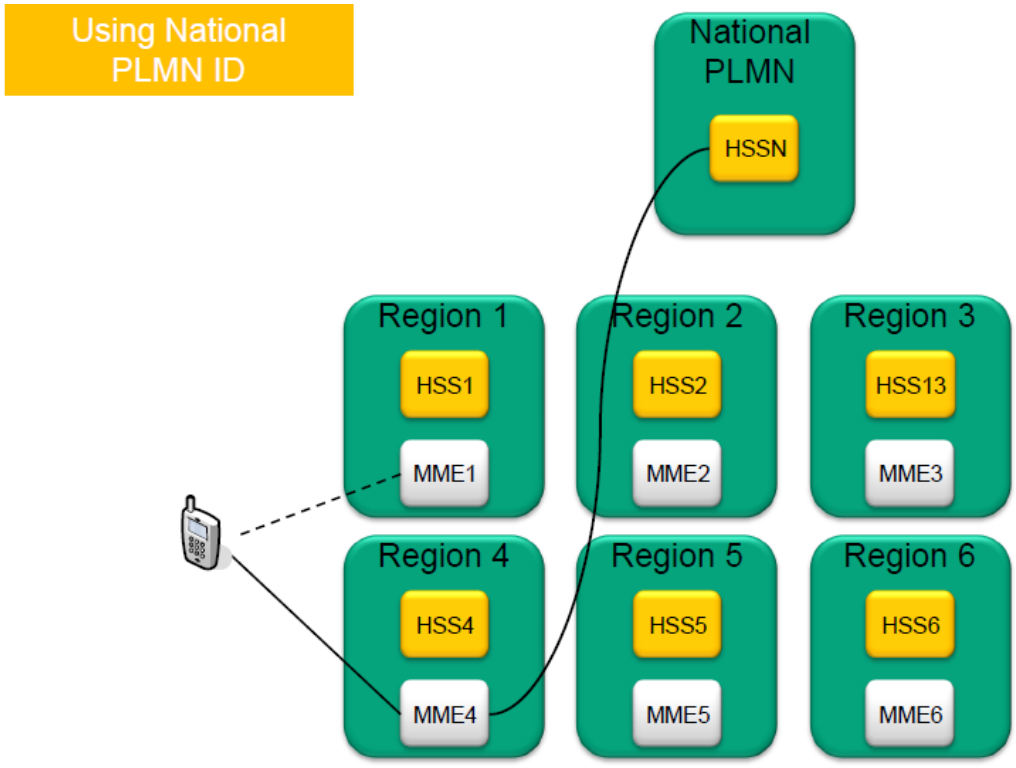
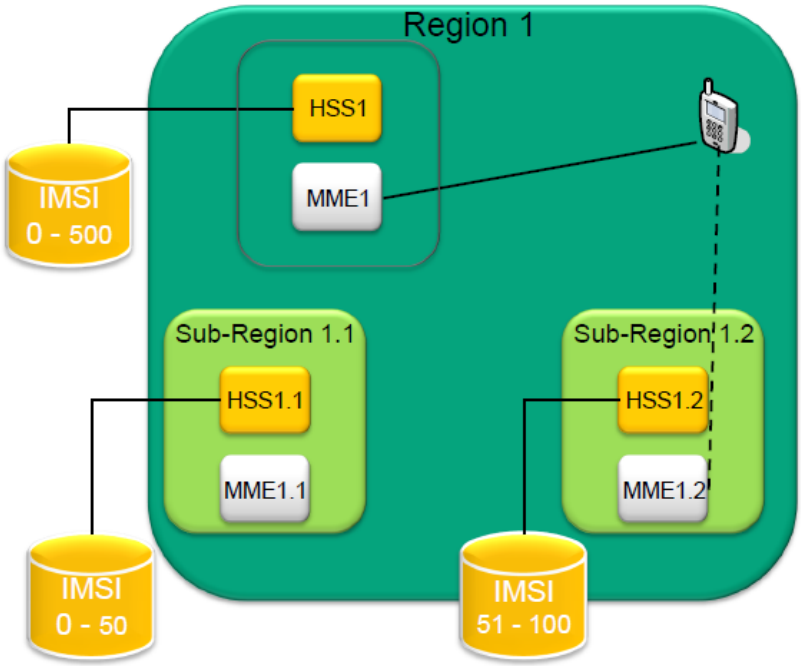


Figure 4



C. Open Standards.

Harris is fully supportive of the use of mandated open standards for IP transport and strongly supports the adoption of the LTE standard.[5] Harris believes that the Commission should be involved in setting overall capabilities of the network and critical interoperable applications. However, the Commission should not attempt to codify the specific technical requirements needed to implement applications. Such activity should be left to appropriate standard setting organizations. The Commission should limit its mandates to those required to facilitate, as defined by the NSPSTC report, "routine use" of home applications while roaming, and "mutual aid use."[6]

[5] Id. at ¶ 27.

[6] *See* National Public Safety Telecommunications Council, "700 MHz Broadband Task Force Report and Recommendations" (Sept. 4, 2009), *available at* http://www.npstc.org/documents/700_MHz_BBTF_Final_Report_0090904_v1_1.pdf ("NPSTC BBTF Report").

D. Roaming.

Public safety networks that conform to the LTE standard should have the inherent capability to provide roaming with commercial carriers that also conform to the LTE standard. In order to ensure public safety operators can interoperate with commercial networks, the public safety operator would have to engage in a roaming agreement and perform roaming tests with the commercial operator. Harris believes that public safety operators should determine whether or not to establish roaming agreements with commercial operators based on their operational requirements. However, the Commission should establish a framework that would presume inter-network roaming and facilitate the establishment of good faith roaming agreements.

Harris agrees with the Commission's conclusion regarding direct interconnectivity between networks.[7] While it may be cost effective to implement a direct connection in high inter-regional traffic situations, it is not cost effective for a scalable interconnection solution. Harris does not recommend the use of the public Internet for interconnection among regional or tribal networks.[8] While there are security solutions that may be employed over the public Internet it does not provide the level of reliability and performance required by public safety roaming users. Harris believes that third party network operators have the capability to provide interconnectivity links between networks with the required performance, security, and reliability to accommodate public safety's needs. The selection and number of vendors is a question that should continue to be evaluated as networks are deployed.

[7] *Fourth FNPRM*, *supra* note 5, at ¶ 39.

[8] *See* Id. at ¶ 40.

Harris also supports the Commission's tentative conclusion to have all public safety broadband networks support home-routed and local breakout roaming.[9]

E. Out-of-Band Emissions and Related Requirements.

Harris agrees with the Commissions tentative conclusion to adopt the OOBE in the Waiver Order for the nationwide wide network.

- On any frequency outside the 763-768 MHz band, the power of any emission shall be attenuated outside the band below the transmitter power (P) by at least 43+10 log (P) db; and
- On any frequency outside the 793-798 MHz band, the power of any emission shall be attenuated outside the band below the transmitter power (P) by at least 43 + 10 log (P) db.[10]

F. Applications.

Harris agrees with the Commission's recommendations to define a minimum set of applications and require support for the following five applications to facilitate roaming across public safety broadband networks:

(1) Internet access;

(2) Virtual Private Network (VPN) access to any authorized site and to home networks;

(3) A status or information "homepage;"

(4) Provision of network access for users under the Incident Command System (ICS); and

(5) Field-based server applications.[11]

[9] *See* Id. at. ¶ 35.

[10] Id. at ¶ 51.

[11] Id. at ¶ 55.

At this time the Commission should not require any additional base line standards, but should create an environment that is conducive to the development of new applications.[12] This can most effectively be accomplished through the vendor community and through designated standard setting bodies. Harris does not believe that other applications should be mandated at this time. Mandating a large number of applications, especially based on a technology that is still in development, is premature. In particular, some of the features are not likely to be in the first commercial LTE releases, and other features are more appropriate to commercial carriers with legacy 2G/3G networks, which may not be optimal for public safety.

In addition, some of the features described in the BBTF Report were defined under the assumption of a commercial carrier providing the complete network and may not provide an optimal implementation for public safety. For example, in *Section 6.3.2.4 Text Messaging*,[13] the BBTF Report proposes using 3GPP TS 23.204 V8.4.0 and 3GPP TS 24.341 V8.1.06 for SMS support. This method is based on the assumption that the network is deployed by a carrier with a legacy SMS system. However, this may not be the optimal approach for a Greenfield system deployed through the waiver process by an entity that does not have a SMS system.

In the case of a public safety system, SMS support could be provided through a more straightforward and cost effective implementation because a public safety LTE system may have the option of delivering SMS using the mechanism defined in 3GPP. These mechanisms include SMS over IP, as specified in 3GPP TS 23.204 and 3GPP TS 24.341, and SMS over SGs, as specified in 3GPP TS 23.272. Either of these approaches provides a solution for both the full IMS based LTE network, as well as, a solution for networks that have a legacy SMS delivery mechanism in place. The analysis of *Sections 6.3.2.4 and 6.3.3* of the BBTF Report demonstrates

[12] *See* Id. at ¶ 56.

[13] *NPSTC BBTF Report*, *supra* note 6, at 21.

the need for caution when mandating applications, especially as the LTE standard is a rapidly evolving.

Encouraging innovation and regional flexibility in initial deployments is the best way to determine what exact requirements should be a part of the framework for the PSBN. ERIC, in coordination with other public safety technical bodies, will serve as good outlets to collect and dissect information. The Commission should be wary of mandating applications in such a rapidly changing environment. Harris notes that flexibility and interoperability are not inherently mutually exclusive concepts so long as the Commission sets an overarching framework—as it is currently doing. Flexibility can provide public safety users to implement new applications without the need for regulatory action by the Commission.

G. Interconnection with Legacy Public Safety Networks.

The ability to interconnect users of the public safety broadband network to users of legacy narrowband networks will be critical to the adaption of broadband networks. [14] The issues involved in voice interconnection are substantially different from those of data interconnection, and should be considered separately. In the case of data, narrowband networks, by definition, support very low effective bit rates and long packet acknowledgement delays relative to broadband networks. Therefore, direct IP interconnection of narrowband and broadband networks creates a very real risk of flooding the narrowband networks with excessive quantities of data. Any gateway device intended to bridge data traffic between legacy and broadband networks must, therefore, have effective data throttling capabilities. In general, Harris believes that mandated "data interoperability" between broadband and narrowband is not a requirement – as there is not a uniform set of applications that can be or need to be run on these networks. Agencies that desire data interconnection between narrowband and broadband

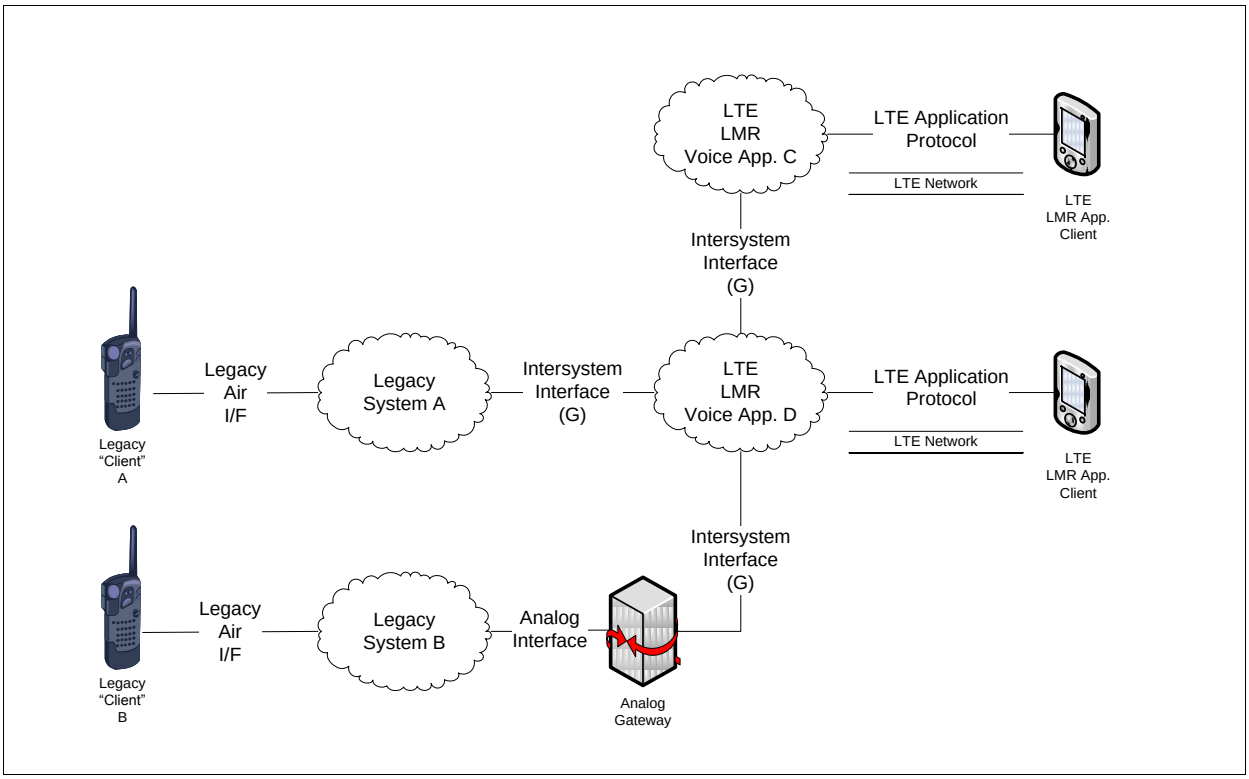
[14] *See Fourth FNPRM*, *supra* note 12, at ¶ 58.

networks can run applications or middleware that ensure that the applications run adequately over both networks.

Interoperability of voice, and particularly PTT voice, requires a separate analysis. The ability to interconnect legacy systems with new technology greatly facilitates the transition from the old to new systems. The primary disadvantage being that some late adopters feel less pressure to transition then they might in systems without legacy interoperability. Advantageously, however, support for legacy operations allows users to spread their capital investment over time, particularly in user devices, and to make the transition in manageable groups rather than in mass.

From a technical perspective, Harris supports a view of analog and digital legacy voice services as applications providing services to PTT clients. When a PTT application is standardized for LTE, it is likely to provide a superset of the same services. Bridges between these services should be provided via an inter-system (G) application interface. This approach is illustrated in Figure 5. Today, all major P25 infrastructure vendors support such an interface, the P25 Inter-subsystem Interface (ISSI). Harris recommends the use of the P25 ISSI as the interface between narrowband and LTE systems, and that vendors provide voice over LTE solutions that can communicate with P25 users over the ISSI.

Figure 5



H. Network Capacity.

Implementation of the public safety broadband network will likely result in capacity that is dependent on the individual regional use cases. For example, in a rural system, with large coverage areas, the capacity of the network might be lower as users that use network resources have an average lower signal quality and thus operate at a lower modulation index. In an urban network, the capacity may be higher as users are more typically near the site and are able to access the high throughput modulations. Moreover, in many networks, the actual capacity of some sites might be throttled by the available backhaul bandwidth. It would not be prudent for the Commission to codify capacity requirements as they will vary greatly from deployment to deployment. Further, requiring a minimum backhaul capacity may limit deployments to rural or remote areas that could still have value with a lower capacity site (as opposed to not having a site). Harris recommends that roaming users be provided with an understood set of network

services, and that the details of these services be defined through a suitable inter-regional governance structure.[15]

I. Security and Encryption.

Harris applauds the Commission's attention to this critical issue both in terms of this proceeding[16] and in the creation of the ERIC PSAC Security and Authentication Working Group. Harris believes that development of a comprehensive security architecture, driven by suitable governance structure is critical to success of the public safety broadband network. Development of the architecture and governance structure should be based on well established Information Assurance ("IA") principles, driven by clearly articulated objectives. Harris believes that the following IA principles should form the backbone of the security and encryption framework:

(1) Risk Assessment – Understanding the risks and costs associated with the capabilities and limitations of the security system(s).

   a. The push towards mission-critical use of the PSBN will bring increased risk.

   b. Mission critical public safety networks must work when nothing else does – the public safety mission is to protect life and property

(2) Threat – Understanding the nature and types of attacks that the PSBN will experience. For example the following well-know types of threats are addressed in the LTE baseline, along with others not listed here:

   a. Denial of Service (DoS) attacks.

   b. Theft of Service (TOS).

   c. IP address spoofing.

   d. User ID theft.

[15] *See* Id. at ¶ 64.

[16] Id. at ¶¶ 65-69.

e. Intrusion Attacks.

f. Bidding down a negotiated security policy.

(3) Vulnerability – Understanding and protecting vulnerable points within the nationwide public safety broadband network—both technological and those driven by governance and policy.

a. The LTE network will be open to many users.

b. Many applications will operate over the network.

c. Access to the Internet will be provided.

d. Large emerging eco-system of devices with a variety of computing environments will emerge.

e. The nation-wide Public Safety Broadband network will be a frequent target of attack.

f. Commercial LTE will be a frequent target of attack - success may impact the public safety broadband network due to use of a common LTE standard.

Ultimately the public safety broadband network security policy must be driven by a suitable governance organization(s) that drives implementation based on its key objectives. As a baseline, Harris proposes the following objectives:

(1) Availability: Ensure that network services are not disrupted by malicious attacks.

(2) Interoperability: Ensure that security mechanisms do not inhibit interoperability.

(3) Privacy: Ensure protection and integrity of sensitive data and identities.

(4) Usability: Ensure that security-enabled devices and services are easy to use.

(5) QoS: Ensure that security mechanisms are not detrimental to achieving QoS required for mission critical applications.

(6) Cost Effective: Ensure that the cost of implementing security is consistent the cost associated with security risk.

(7) Standards Based: Use of robust standards should form the basis for implementing and IA framework.

Built on this framework and key objectives, Harris supports the following positions:

(1) Requirement of the three Network Domain security layers as specified in 3GPP TS 33.401 and as referenced in the NPSTC BBTF Report.[17]

(2) Use of 128-EEA2 and 128-EIA2 both of which are based on AES 128-bit algorithms and as specified in 3GPP TS 33.401.

(3) Implementation of Network Security Domains consistent with 3GPP TS 22.210 which defines profiles for IPSec and IKE. Note that User Equipment ("UE") does not participate directly in the network security domain and therefore does not need additional information to operate within a network that employs a network security domain. Network security domains that terminate at the Security Gateway ("SEG") within an operator or regional network should have no impact on interoperability between network operators and external packet data networks.

(4) Application Domain Security as specified in 3GPP TS 33.102 and 3GPP TS 22.101 is a value added feature that may be required by certain portions of the public safety community. Mandating these capabilities will likely have an impact on the availability and cost of end user devices and applications. Harris recommends that when public safety jurisdictions implement Application Domain Security, they do so in accordance with the standards referenced above. As such, operators of public

[17] *NPSTC BBTF Report*, *supra* note 13.

safety broadband networks and/or providers of applications should be required to support these capabilities.

(5) Visibility and Configurability of Security as specified in 3GPP TS 33.102 and 3GPP TS 22.101 is notionally consistent with certain established policies and procedures used in public safety today. For example, notification to a user that a particular radio talk group is secure vs. not secure is a requirement imposed on some public safety communication systems today. In keeping with this notion, Harris recommends that when a jurisdiction is required to implement a Visibility and Configurability function, it does so in accordance with the 3GPP standards noted above. As such, operators of public safety broadband networks should be required to support these capabilities.

Finally, Harris notes that since ever-more sophisticated attacks will emerge in the future, the Commission must implement a flexible regulatory framework that permits continued evolution of the security architecture and governance structure as we deal with future threats and vulnerabilities. Continued reassessment of the risk cost/benefits of security will be essential to protecting this vital national asset.

J. Robustness and Hardening.

Given the mission-critical nature of the public safety broadband network, it is essential that its implementation be consistent with robustness and hardening best practices used in public safety today. Harris urges that the Commission recognize that regional differences in hardening practices are important, particularly when looking at areas of the country that are prone to hurricanes, tornadoes and/or earthquakes. Local jurisdictions are best suited to understanding these nuances and the Commission should not mandate a particular implementation nation-wide.

That said, Harris agrees with the Commission that the public safety broadband network requires power back-up and contends that the most serious incidences can extend far beyond 8 hours.[18] A properly designed power back-up system provides an uninterruptable power system ("UPS") that generally consists of battery back-up for immediate carry over, followed by a longer duration power source traditionally a diesel generator that comes on line following power interruption that exceeds several seconds. Major incidences like Hurricane Katrina have shown that additional requirements beyond time duration are important to insuring that back-up power services are available when they are most needed. Harris makes the following recommendations with regards to back-up power requirements that the Commission must consider when establishing rules:

(1) Back-up power needs to be truly autonomous with several days of fuel stored on site. In the worst of disasters, infrastructure such as gas and fuel lines may be either damaged or shutdown for safety reasons; and

(2) Power back-up systems need to be protected from flooding. Appropriate criteria are likely to be implemented on a regional.

K. Coverage Requirements.

Harris believes that not all jurisdictions should be subject to the same requirements for coverage and performance.[19] In particular, high density population centers should have system designs that carry the required traffic for day-to-day operations with the additional capacity to handle routine emergency response or response to large scale events. A side effect of these capacity constraints may be that urban systems will have to support data rates that exceed the minimum over nearly all of the served area.

[18] *Fourth FNPRM, supra* note 16, at ¶ 70.

[19] *See* Id. at ¶ 71.

Rural areas may greatly benefit from the availability of a broadband network even if that network does not achieve the targeted data rate across much of a rural jurisdiction's area. Harris understands that some level of nation-wide conformance is required to ensure local optimization does not compromise the overall objective of achieving nation-wide interoperability of the public safety broadband network.

Requirements on coverage and capacity can dictate the way in which public safety broadband is rolled out. Two potential models for a rollout include: (1) an area maximizing approach in which public safety entities attempt to make maximum use of their existing infrastructure; and (2) an approach in which higher site densities are required to meet coverage and performance benchmarks. In the first approach, public safety entities utilize existing site locations and operate a system that may not have continuous coverage, but that provides rural areas with broadband services at locations that rapidly become known to system users. While this approach might be appropriate for a data-only network operator, it would not likely be appropriate for a critical voice user. In the second approach, where coverage and performance benchmarks must be met over a continuous area, new site development and its costs will pace the deployment of broadband systems. Therefore while the definition of coverage can be defined as minimum rates with 95% edge reliability, this specification should not be interpreted to require continuous coverage in rural areas, but instead to act as a uniform definition of coverage.[20]

L. Coverage Reliability.

Unlike narrowband systems (traditionally referred to as Land Mobile Radio ("LMR") Systems) that have a somewhat straightforward coverage definition, LTE coverage is complicated because it depends on the data rate and the network load. Coverage of the network

[20] *See* Id. at ¶ 72.

varies depending on the number of users, what those users are doing, and how much data is being consumed. Further, the coverage varies as a function of data rate. Currently coverage for narrowband public safety spectrum is not mandated and left to the local user to optimize based on operational needs and economic constraints. A given jurisdiction may have varying coverage needs. There may be regions of the jurisdiction that it is cost prohibitive to provide coverage at some pre-determined cell edge capacity. There may be areas that it makes sense to cover, but at a lower effective data rate than has been discussed to date (768 kbps on DL and 256 kbps on UL).

Due to the complexity of LTE coverage prediction, the Commission, through a standards setting process, should create a standard "definition" of coverage—such as the 95% reliability definition referenced to in the Commission's December Wavier Interoperability Order.[21] In narrowband LMR systems, this coverage definition is defined by the TIA document TSB-88. By creating a standard for how coverage is discussed and evaluated, users can have a uniform understanding of what the network coverage is. As the network is built out, Harris recommends that the Commission create a process for regional entities to submit to the Commission the land areas inside their network where they have "coverage" as defined above.[22] With this information, relevant parties will be able to understand the coverage of the network and thereby be capable of assessing its vulnerabilities and potential need for further investment in build-out.

[21] Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks, PS Docket No. 06-229, Order, DA 10-2342 ¶ 24 (rel. Dec. 10, 2010).

[22] *See Fourth FNPRM*, *supra* note 20, at ¶ 75.

M. Interference Coordination.

Both 700 MHz narrowband and 700 MHz broadband need to be protected from interference from neighboring frequency allocations, and each other.[23] The Commission must continue to support and protect mission critical voice systems, which remain the life blood of public safety communications. While public safety broadband technology continues to evolve and move towards a converged voice and data environment, narrowband voice communications currently supply public safety with geographic coverage and reliability vastly superior to current public safety broadband capabilities. Although the benefits of public safety broadband will be enormous, deployment must not be completed at the detriment of mission critical voice operations. Prior to deploying a broadband network, public safety entities should be required to coordinate their deployments with existing and planned narrowband network operators (and visa-versa).

Narrowband is adjacent to public safety broadband and consequently it must be protected from interference by LTE transmissions. For cooperating jurisdictions, common site locations for narrowband and broadband public safety sites is a highly effective method to reduce interference. Where common sites are not possible, system designs should include the effects of adjacent allocations into the system design to ensure adequate protection.

The potential for adjacent or alternate channel interference is not limited to "subsequent phases"[24] of LTE public safety deployments, instead it is a reality through all phases of deployment. Traditional public safety narrowband systems are designed with high performance base stations, mobile, and portable receivers that are intended to reject adjacent channel energy. These systems operate in frequency bands where there is coordination between narrowband

[23] *See* Id. at ¶¶ 80-84.

[24] Id. at ¶ 79.

channel licensees. A side effect of this legacy paradigm is a requirement that transceivers have very high performance RF specifications to enable disparate systems to operate on adjacent channels without causing significant interference. This inherent high performance requirement drives equipment cost and should be avoided for LTE deployments. Interference from cellular systems in the 800 MHz band is an example where even high performance receivers were not sufficient to overcome interference issues caused by systems that implemented a higher density of sites than public safety. In addition, even with these high performance requirements, there is no guarantee that a system will not have interference due to a particular real world deployment scenario.

Interference from adjacent channel systems in narrowband or broadband systems generally result from near and far situations. For example, a nearby frequency offset base station causes enough interference to a receiving device that it can no longer receive a signal from its relatively distant serving base site. For commercial deployments 3GPP has addressed this issue under its own set of presumptions that is sufficient for carrier grade LTE services. Harris does not believe these protections, based on the presumptions set forth by 3GPP, are sufficient to shield public safety networks from harmful interference.

Public safety systems are inherently different in their mission, funding, scale, and criticality. By adopting LTE as the public safety broadband standard, benefits are reaped through leveraging commercially developed network Cores, radio access equipment, and user equipment. However, simply deploying commercial equipment will not result in a public safety grade broadband communication system. Protection mechanisms must be in place to ensure system interference is mitigated where and when it occurs.

Public safety broadband and commercial cellular both use LTE for their radio access network and consequently the physical interference mechanisms are bi-lateral for similar deployment densities. However, commercial carriers will serve a much large user base than public safety systems and will therefore build out a higher site density. In areas where the commercial site density is higher than public safety, LTE co-location is not possible at all commercial sites and therefore the potential exists for interference.

LTE introduces self optimizing network ("SON") procedures as a cornerstone of its requirements. SON is seen as a tool to enable network operators to improve network efficiency by enabling system parameters to be automatically adjusted according to capacity demands and changes in RF propagation. As a result parameters that have been traditionally fixed in wireless systems like antenna patterns, EIRP, and bandwidth become dynamic. Likewise, interference when it occurs may be dynamic. Agreements between adjacent operators may require optimization of SON processes to prevent interference from occurring as a consequence of automatic network adjustments.

Harris does not believe that it is in the best interest for the Commission to implement technical rules that shield public safety bands from interference by requiring difficult performance standards on public safety bands and its adjacent bands. Instead protection is best obtained by anticipating interference issues and planning ways to avoid them, rather than focusing on reactive measures to address issues when they happen. For this reason, the Commission's rules should require that 700 MHz public safety and commercial broadband operators to share within 30 days of a request, detailed site information with public safety operators and their contractors for the purpose of analyzing and eliminating interference during system planning, implementation, and maintenance phases. SONs will complicate interference

coordination by requiring analysis of parameters over their range rather than a fixed value. Examples of information that should be shared includes, but is not limited to, site locations, EIRP, antenna patterns, signal bandwidth, and signal type. To ensure continuing interference abatement to acceptable levels, commercial and public safety operators once entered into an agreement must inform each other of their intention to add sites or change the range of adjustment of system interference coordination related parameters.

N. In-building Communications.

The comprehensive implementation of in-building communications is an affordability issue. The Commission should not mandate what RF margin is provided as raising that bar too high will delay the deployment of the technology. Network operators may choose to build networks with little in-building coverage and later expand to add additional RF margin, for example to support voice communications to hand-held devices. Network operators should be allowed to implement networks based on this deployment paradigm.[25]

Distributed antenna systems have been successfully used for years (especially in tunnels) and provide coverage where it might not be otherwise. This is true for both commercial as well as narrowband public safety networks. The Commission should continue to allow for the use of distributed antenna systems.[26]

[25] *See* Id. at ¶¶ 123-124.

[26] *See* Id. at ¶ 125.

O. Deployable Assets.

The Commission should permit the use of 4.9 GHz and satellite bands. The 4.9 GHz band could be useful for public safety entities backhaul needs. Network operators should be provided the greatest spectral flexibility to rapidly implement deployable assets.[27]

P. Operation of Fixed Stations and Complimentary Use of Fixed Broadband Spectrum.

The Commission should allow public safety entities to operate fixed use on an ancillary basis in the 700 MHz public safety broadband spectrum. As pointed out by the Commission "enabling such ancillary fixed use will ensure that the spectrum remains available for its primary purpose while allowing users appropriate flexibility."[28] Having spectrum available for fixed uses is important for public safety surveillance and backhaul services.[29] In addition, the Commission should implement rules that allow public safety entities to utilize the 4.9 GHz and 700 MHz bands as complimentary. The 4.9 GHz band could be a vital resource to public safety in providing 700 MHz backhaul services. Rules that allow 4.9 GHz networks to compliment 700 MHz networks will maximize the capabilities and capacity of both bands.

Q. Public Safety Broadband and NG 911.

Harris supports the continued development of LTE technology as both appropriate for the public safety network and as applicable to IP and telecommunications industry standards.[30] By maintaining its link to commercial LTE developments, and assuring the continued development of open standards, the public safety broadband network maximizes both its utility in addressing communications such as NG 911 and ensures a seamless deployment and development of the

[27] *See* Id. at ¶ 128.

[28] Id. at ¶ 129.

[29] *See* Id. at ¶ 130

[30] *See* Id. at ¶ 133.

network. The Commission must resist the lure of "special" public safety communications that do not conform to the LTE Standard, or it will lead to a "proprietary" public safety communications network.

IV. HARRIS SUPPORTS FEDERAL ACCESS AND USE OF THE 700 MHZ PUBLIC SAFETY BROADBAND SPECTRUM IN FURTHERANCE OF INTEROPERABILITY.

Access to the national public safety broadband network by federal entities is in furtherance of the overarching goal that the network is both nationwide and promotes interoperability across public safety users—both inter and intra jurisdictionally. Harris supports federal user access and believes that the Commission's interpretation of Section 2.103 to date is accurate.[31] Federal entities play a vital part of emergency response and coordination, especially in widespread or high impact events.

In order to facilitate federal access Harris supports the use of a national clearinghouse, as recommended by the Commission in the *FNPRM*.[32] Regardless of the approach taken by the Commission for facilitating access, coordination between federal and state and local users is vital. Harris supports the Commission providing states the ability to lease a portion of their spectrum to federal users in furtherance of that state's public safety mission. Such spectrum leasing arrangements may be crucial around federal government venues and along the northern and southern borders. Working through the states will ensure the proper level of coordination takes place between federal and local users. The Commission should provide users (federal and

[31] See Service Rules for the 698-746, 747-762 and 777-792 Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, WT Docket No. 06-150, PS Docket No. 06-229, *Second Report and Order*, 22 FCC Rcd 15289, 15427 n.822 (rel. Aug. 10, 2007) ("*Second Report and Order*"); see also Requests for Waiver of Various Petitioners to allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks, *Order*, PS Docket 06-229, 25 Rcd. 5145, 5155-56, ¶ 34 (rel. May 12, 2010) ("*Waiver Order*") (granting 21 waivers for early deployment in the 700 MHz public safety broadband spectrum and establishing rules for deployment).

[32] *Fourth FNPRM* , *supra* note 30, ¶ 102.

state/local) with the greatest amount of flexibility to determine what access model works best for their particular circumstance. Harris believes that both a spectrum leasing and subscriber model should be permitted. These two models are not mutually exclusive and will allow individual regions to determine what model is best to meet their needs.

Since the greatest burden from Federal users would be on the public safety network in Washington D.C., Harris suggests that the network in Washington D.C. be built and paid for by a federal entity or entities and that the Commission's rules be aligned with that objective. The federal entity or entities would then enter into roaming agreements with peer networks around the country using the same Standard Roaming Agreement outlined by the Commission in the proposed rules.[33] Because of the large number of federal users that will be homed in the Washington D.C. network, Harris suggests that as reciprocity for use of state and local networks, the federal entity or entities would pay for all Clearinghouse costs associated with creating and operating the national network. State and tribal network operators would then know beforehand that they need bear only their own costs and, all national Clearinghouse issues would be handled at the federal level for a national network.

V. PERMITTING ENTITIES THAT SUPPORT PUBLIC SAFETY'S CORE MISSION ACCESS TO 700 MHZ PUBLIC SAFETY BROADBAND NETWORKS IS PERMISSIBLE UNDER SECTION 337 OF THE COMMUNICATIONS ACT OF 1934.

Pursuant to Section 337(f) of the Communications Act of 1934,[34] the Commission should permit public safety entities the discretion to provide access to public safety broadband networks for users and entities that support public safety's mission. While first responders should remain the primary users and "licensees" of the spectrum, discretion should be provided to the first

[33] Id. at ¶ 99.

[34] 47 U.S.C. § 337(f); *see also* 47 C.F.R. 90.523.

responder community to determine what other government and quasi-government organizations would advance the mission of public safety and should be permitted network access on a secondary basis. Harris does not agree with the Commission's restrictive definition of network access adopted in the *Waiver Order.*[35] The Commission's definition limits the establishment of beneficial partnerships for public safety and public safety's ability to work with other government and quasi government entities to protect the safety of life, health, and property.

An overly narrow interpretation of Section 337 would limit the establishment of beneficial partnerships between public safety and other non-public safety government and quasi-government entities who have similar mission critical communication needs and requirements. Access to public safety broadband networks by entities that would advance the core mission of public safety, such as transportation entities and critical infrastructure providers, offer public safety the opportunity to obtain independent funding, and reduce overall deployment costs through leveraging existing infrastructure. Obtaining independent sources of funding and leveraging existing infrastructure are key are Commission goals that were advocated for in both the *700 MHz Second Report and Order*[36] and the National Broadband Plan.[37] In addition, public

[35] In the Commission's *Waiver Order* the Commission chose to adopt its tentative conclusion's set forth in the Third Further Notice of Proposed Rulemaking and "limit the use of the 700 MHz spectrum to entities whose 'sole or principal purpose' is 'to protect the safety of life, health, or property' and who meet the remaining requirements of Section 337(f)." *Waiver Order*, *supra* note 31, at 5155, ¶ 34; *See* Service rules for the 698-746, 747-762 and 777-792 MHz Bands; Implementing a Nationwide, Broadband Interoperable Public Safety Network in the 700 MHz Band, *Third Notice of Proposed Rulemaking*, WT Docket No. 06-150; PS Docket No. 06-229, 23 FCC Rcd. 14301, 14404-14407 ¶¶ 322-327 (rel. Sept. 25, 2010) ("*Third FNPRM*").

[36] "Providing the D Block licensee with the opportunity to offer commercial services on this spectrum, on a secondary basis, is an integral part of a viable framework for enabling the 700 MHz Public/Private Partnership to finance the construction of a nationwide, interoperable public safety broadband network." *Second Report and Order*, *supra* note 31, at 15437, ¶ 416.

[37] The Commission noted in the National Broadband Plan that providing critical infrastructure users, such as utilities, secondary spectrum access to the 700 MHz public safety broadband spectrum "serves the added purpose of allowing the public safety licensee(s) to leverage infrastructures that utilities might currently have. Therefore, access to utilities' towers and other structures may be part of any secondary usage program." Report to Congress, A National Broadband Plan for Our Future, Federal Communications Commission, pg. 328, fn. 7. (rel. Mar. 16, 2009).

safety, transportation entities, utilities, and other critical infrastructure entities must reach all citizens, regardless of their location, and are increasingly relying on access to broadband communications technology. Promoting collaborative deployment efforts that utilize shared resources while still advancing the public interest should be encouraged by the Commission.[38] Therefore, the Commission should allow public safety entities the ability to grant spectrum access to critical infrastructure entities on the condition that the spectrum is used to further the public safety mission.

When permitting secondary use, the Commission should not adopt specific usage limits for secondary use of the spectrum. Rather, public safety entities themselves are best suited to determine whether limits on secondary use would be necessary to preserve spectrum capacity for public safety. The Commission could ensure that the public safety broadband spectrum is being utilized in accordance with Section 337(f) by requiring public safety entities to enter into a "Sharing Agreement" or a "Memorandum of Understanding" with any permissible secondary users—as is similarly required in the 4.9 GHz band[39] and under the 700 MHz private-public partnership rules.[40] Public safety entities should also be permitted to set reasonable user access fees as part of the Sharing Agreement, either on a subscription or in-kind basis. While the Commission should require that revenue collected from user access fees be used to enhance or fund the operation of the public safety broadband network, the public safety entity collecting the user access fee should be allowed to utilize the revenue as it sees fit to fulfill that requirement.

---

[38] *See e.g.*, Las Vegas Metropolitan Police Department, Washoe County Sheriff's Department, the Washoe Regional Communications System, the Nevada Department of Transportation, and NV Energy, representing the State of Nevada 700 MHz Broadband Wireless Network (SONNet), *Request for Waiver – Expedited Action Requested* (filed May 13, 2010).

[39] *See* 47 C.F.R. § 90.1410 and § 27.1310 (2009) (establishing the terms and conditions for the relationship between the Upper 700 MHz D Block licensee and the Public Safety Broadband Licensee).

[40] *See* 47 C.F.R. § 90.1203(b) (2009)(allowing the establishment of sharing agreements for use the 4.9 GHz band by non-public safety entities that operate in support of public safety).

A. Commission Oversight of Secondary Network Access Can Be Accomplished Through the Establishment of Network Sharing Agreements.

To ensure that the public safety broadband spectrum is not utilized for purposes outside the scope of Section 337(f) the Commission could require that a Sharing Agreement be filed with the Commission and Public Safety Broadband Licensee within a reasonable time period following the establishment of the Sharing Agreement. The Sharing Agreement should not be subject to prior Commission approval, but its filing would provide the Commission with the necessary oversight to ensure that the public safety broadband spectrum is being used in accordance with Section 337. Additionally, the Commission could establish required information that must be included in the Sharing Agreement, such as:

(1) Governance Structure

(2) Network Access Terms and Conditions

(3) Identification of Use Cases by Secondary Users

(4) Intra and Inter Jurisdictional Geographic Coordination Requirements

(5) Interference Mitigation Plans

(6) Compliance with the Public Safety Spectrum Trust De Facto License

(7) User Access Fee Structures (Subscription or In-Kind)

(8) A commitment to reinvest any revenue into the operation, maintenance, build-out, enhancement or usage of the public safety broadband network.

B. The Commission Should Allow Public Safety Entities to Set Reasonable Spectrum Access Fees And Utilize Revenue to Enhance the Network.

Harris believes that secondary users can be charged a fee for access to the network without violating Section 337. For example, the *Second Report and Order* found that service fees for commercial networks using the spectrum should be specified in the network sharing

agreement.[41] Similarly, the regional and local network operators should negotiate access fees with utilities and critical infrastructure entities, and include a fee structure in the network sharing agreement. The Commission should ensure that the fee structure in the network sharing agreements terms and conditions is both reasonable and predictable[42] through its oversight authority.

Regardless of whether payments are made via in-kind contributions or cash payments, Section 337 is not violated. As long as the access fees established in the network sharing agreement are reasonable the method of payment that the secondary users choose to use would be consistent with the parameters established under Section 337. The terms and conditions of the network sharing agreement should govern any fees associated with network access. Since each geographic region faces unique public safety needs, public safety entities are better suited than the Public Safety Broadband Licensee to establish sharing agreements, set fees and determine how to allocate revenue to enhance the public safety broadband network.

While Harris believes that the Commission should require revenue collected from spectrum access fees be reinvested into the operation, maintenance, build-out, enhancement or usage of the public safety broadband network, public safety entities collecting the fees should be left to determine how to best enhance the network in their jurisdiction. The Commission should not require that any revenue generated by access fees to be paid to the Public Safety Broadband Licensee. Through its oversight authority of the network sharing agreement, the Commission can ensure that the terms and conditions do not include any unreasonable access fees or use of revenues generated by access to the network.

[41] *Second Report and Order*, *supra* note 36, at 15448, ¶ 450.

[42] *See Third FNPRM*, *supra* note 35, at 14424, ¶ 388.

C. Permitting Secondary Use of the 700 MHz Public Safety Broadband Spectrum is Permissible Based on Previous Commission Interpretations of Section 337.

A flexible interpretation of Section 337(f) is consistent with the Commission's findings in the following proceedings: (1) the 700 MHz proceeding; (2) the National Broadband Plan; and (3) the 4.9 GHz proceeding.

1. 700 MHz Proceeding

Prior to the Commission's narrower interpretation of network access adopted in the *700 MHz Third Further Notice of Proposed Rulemaking* ("*Third FNPRM*"),[43] the Commission had a broader view of network access in the 700 MHz public safety spectrum band. For example, in the Commission's *700 MHz Second Further Notice of Proposed Rulemaking* the Commission noted that "pursuant to the statutory definition, a service can still be considered a "public safety service" even if its purpose is not solely for protecting the safety of life, health or property, so long as this remains its principal purpose."[44] In addition, the Commission's interpretation of Section 337(f) supported providing public safety with discretion to determine who should be given access to PSBNs. Given the importance of the 700 MHz spectrum allocation to public safety and finite amount of spectrum, the Commission believed that it was "unlikely that the intended scope of authorization from such governmental entity or entities would include providing spectrum access, even on an occasional or limited basis, to entities that do not provide public safety services."[45]

While during the course of the 700 MHz proceeding the Commission deviated from its earlier interpretations of Section 337(f) outlined above, the conclusions made in the *Third*

[43] Id. at 14404-14407, ¶¶ 322-327.

[44] Service rules for the 698-746, 747-762 and 777-792 MHz Bands; Implementing a Nationwide, Broadband Interoperable Public Safety Network in the 700 MHz Band, *Second Further Notice of Proposed Rulemaking*, WT Docket No. 06-150, PS Docket No. 06-229, 23 FCC Rcd. 8047, 8061 ¶ 30 (rel. May 14, 2008).

[45] Id. at 8062, ¶ 32.

FNPRM were only tentative, and the Commission can still and should change direction. The circumstances under which the Commission made its tentative conclusions in the *Third FNPRM* have changed dramatically. From a policy perspective the Commission, as a result of the National Broadband Plan, has been attempting to find ways to most effectively leverage existing resources (both spectrum and infrastructure) to provide broadband access not only to consumers, but in support of numerous societal benefits including public safety, energy, and healthcare. As a result of the economic downturn local and state governments, including public safety departments, are cash and resource strapped. Pooling resources to advance important public works projects, such as the deployment of a PSBN, have become an important tool in moving vital projects of great public interest forward. The Commission's conclusions in the 700 MHz proceeding regarding network access to public safety broadband spectrum prior to the *Third FNPRM* are more appropriate today based on the current set of circumstances that waiver grantees and Petitioners find themselves, than the Commission's tentative conclusions in the *Third FNPRM*.

2. National Broadband Plan

In the National Broadband Plan the Commission advocated for providing public safety entities discretion to determine whether to provide non-public safety partners use of the 700 MHz public safety spectrum on a preemptable, secondary basis through leasing or similar mechanisms.[46] In particular, the Commission supported providing utilities access to public safety broadband networks for mission critical communications.[47] The Commission recognized the importance of providing partners, such as critical infrastructure users, access to the 700 MHz

[46] National Broadband Plan for Our Future, Federal Communications Commission, supra note 37, pg. 315 (rel. Mar. 16, 2009).

[47] Id. at 269.

public safety spectrum as their work is critical to supporting first responders and will ultimately benefit homeland security and public safety.[48]

Harris agrees with the recommendations the Commission made in the National Broadband Plan providing public safety broadband network access, on a secondary basis, to critical infrastructure providers.[49] Harris also agrees with the Commission that any revenue received by a public safety entity as a result of spectrum access agreements should be used to build or improve the public safety broadband network.[50] Ultimately, providing public safety entities the opportunity to work with non-public safety governmental and quasi-governmental partners, such as both state owned and private utilities, will help reduce deployment costs and provide the opportunity to leverage the infrastructure of non public safety partners for public safety use. Cost reduction through leveraging infrastructure is a key aspect of the Commission's National Broadband Plan proposal for deploying a nationwide PSBN.[51] The Commission could support this proposal by providing waiver grantees the opportunity to partner with and provide spectrum access, on a secondary basis, to non-public safety government and quasi-government organizations.

3. 4.9 GHz Band

The 4.9 GHz band is another example of where the Commission has implemented a flexible approach to public safety spectrum access under Section 337(f) of the Act. In the 4.9 GHz band proceeding, the Commission based its spectrum access rules on the definition of

[48] Id. at 269-271.

[49] Id. at 314.

[50] Id. at 315.

[51] Id. at 271 and 316.

public safety services laid out under Section 337(f) of the Act.[52] In establishing final rules for the band, the Commission stated that access to the 4.9 GHz spectrum should be "sufficiently flexible to provide a variety of entities access to the 4.9 GHz band, particularly if allowing such entities access would increase the effectiveness of public safety communications, foster interoperability and further ongoing and future homeland security initiatives."[53] The Commission determined that "permitting 4.9 GHz licensees to enter into sharing arrangements with entities not eligible for their own license is in the public interest."[54] The Commission went on to state that it would not impose limitations on the type of specific entities that would be eligible to enter in to sharing agreements and would instead "afford traditional public safety providers that are licensed in the 4.9 GHz band flexibility to exercise their discretion regarding what entities in their jurisdiction operation in support of public safety."[55]

While use of the 4.9 GHz public safety spectrum for commercial use is strictly prohibited, under the noncommercial *proviso* of Section 337(f) the Commission has realized that commercial entities, such as private utilities, should not be disqualified from utilizing the spectrum *per se* as a result of their commercial status.[56] However, under the noncommercial

---

[52] *See* In the Matter of The 4.9 GHz Band Transferred from Federal Government Use, *Memorandum Opinion and Order and Third Report and Order*, WT Docket No. 00-32 *18 FCC Rcd 9152* 9158-9163, ¶¶ 15-25(rel. Apr. 23, 2010) ("*4.9 GHz Third Report*").

[53] Id. at 9158, ¶ 16; "As the Commission has noted previously in a separate proceeding, although the primary function of certain organizations, such as the power, petroleum, and railroad industries, 'is not necessarily to provide public safety services, the nature of their day-to-day operations provides little or no margin for error and in emergencies they can take on an almost quasi-public safety function. Any failure in their ability to communicate by radio could have severe consequences on the public welfare.'" Id., at 9162, ¶ 22, *citing,* Implementation of Sections 309(j) and 337 of the Communications Act of 1934, as Amended, *Report and Order and Further Notice of Proposed Rulemaking*, WT Docket No. 99-87, 15 FCC Rcd 22709, 22746 ¶ 76 (rel. Nov. 20, 2000).

[54] Id. at 9162, ¶ 22.

[55] Id.

[56] "For example, a commercial utility company, with appropriate governmental authorization, is eligible to hold licenses for spectrum in the 700 MHz band for use when it provides services to protect the safety of life, health or property that it does not make commercially available to the public." The Development of Operational, Technical

proviso commercial entities are not eligible for licensing or use of the spectrum if the services they are providing are "[made] commercially available to the public, including the provision of public safety radio service to public safety subscribers for a fee."[57] Examples of prohibited commercial entities would likely include commercial network providers that sometimes carry public safety communications over their network.

Access to 4.9 GHz public safety spectrum by non-public safety entities[58] was made contingent by the Commission on the establishment of written sharing agreements and that communications would be "in support of public safety."[59] The Commission, rightfully, did not attempt to categorize "public safety" versus "non-public safety" entities because the Commission believed that (1) "a bright line distinction would be difficult to draw and might unduly inhibit the use of the subject spectrum that could benefit the public welfare"[60] and (2) "that traditional public safety licensees will be in the best position to determine whether certain sharing arrangements would benefit their public safety communications."[61] The Commission's actions in the 4.9 GHz proceeding recognized the importance of providing public safety the opportunity to explore strategic partnerships so long as such arrangements were to enhance public safety's

---

and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, *First Report and Order and Third Notice of Proposed Rulemaking*, WT Docket No. 96-86, 14 FCC Rcd 152, 188 ¶ 72 (1998).

[57] *4.9 GHz Third Report*, *supra* note 55, at 9159, ¶ 17.

[58] Although commercial use of the 4.9 GHz band is prohibited, private companies supporting public safety agencies with critical infrastructure can negotiate sharing agreements with sponsoring government agencies if such use is for the purpose of protecting life, health, and property. For example, based on an examination of 4.9 GHz licenses entities that have been granted a 4.9 GHz license include Transportation Authorities; Police Departments; Fire Departments; Offices of Emergency Management; Emergency Dispatch and Operations; Airport Authorities; Courts; Electric, Water, and Sewage Authorities; Emergency Medical Services; and Port/River Authorities.

[59] 4.*9 GHz Third Report*, *supra* note 57, at 9162, ¶ 22.

[60] Id. at 9162-9163, ¶ 23.

[61] Id. at 9163, ¶ 23.

mission and utilized on a secondary basis.[62] The Commission's actions in the 4.9 GHz proceeding regarding network access should be replicated in the 700 MHz public safety spectrum band.

Harris believes that in the 4.9 GHz band the ability to create flexible spectrum access arrangements for the purpose of advancing public safety communications has been extremely beneficial to supporting the mission of the public safety community and compliant with Section 337(f) of the Act. While the licensing approaches of the 4.9 GHz and 700 MHz band are very different, the public interest benefit provided by flexible spectrum access rules are the same. It would be in the public interest for waiver grantees in the 700 MHz public safety band to be subject to a similar interpretation of Section 337(f) of the Act as the Commission provided in the 4.9 GHz band.

Given the Commission's previous interpretation of Section 337(f) in the 700 MHz proceeding and 4.9 GHz proceeding, coupled with the Commission's recommendations in the National Broadband Plan, it would be appropriate for non public safety government and quasi government organizations, whose goal it is to advance the mission of public safety, to have secondary access to PSBNs contingent on public safety's approval.

VI. Conclusion

For the foregoing reasons, Harris urges the Commission to take into consideration its views in this proceeding. The Commission should continue its work establishing an overarching

[62] "We recognize that some of the public safety entities covered by Section 309(j)(2) of the Act, whose facilities may be directly involved in an emergency, and who provide essential services to the public at large, may also be interested in utilizing the 4.9 GHz band. The very nature of the services provided by these entities involve potential hazards whereby reliable radio communications is an essential tool in either avoiding the occurrence of such hazards, or responding to emergency circumstances. Furthermore, such entities need reliable communications in order to prevent or respond to disasters or crises affecting their service to the public. We also recognize that in the course of their duties, these entities will need to interact with the traditional public safety service providers, and the inability to do so may affect the ability of both groups of public safety entities to fulfill their missions." The 4.9 GHz Band Transferred from Federal Government Use, *Second Report and Order and Further Notice of Proposed Rule Making*, WT Docket No. 00-32, 17 FCC Rcd 3955, 3931 ¶ 33 (rel. Feb. 27, 2002).

regulatory framework. Additionally, the Commission should not lose sight of the importance that a governance structure plays to facilitating interoperability. Harris strongly encourages the Commission to leave the establishment of specific technical capabilities to the industry through designated standard setting organizations. To encourage interoperability across mission critical communications within a jurisdiction, the Commission should permit access to federal users and determine that Section 337 permits network access to entities that act in support of public safety's core mission (*i.e.*, to protect the safety of life, health or property). Public safety entities on a regional or local basis should be allowed to enter into sharing agreements with authorized secondary users and determine how fees should be used to advance the capabilities of the public safety broadband network. Harris looks forward to working with both the Commission and the public safety community to deploy an interoperable nationwide PSBN.

Respectfully submitted,

HARRIS CORPORATION
600 Maryland Avenue, S.W.
Suite 850E
Washington, D.C. 20024
(202) 729-3700

_____/s/_____

Dr. Dennis Martinez
Chief Technology Officer
RF Communications Division
Harris Corporation

Gregory Henderson
Director, Broadband Products
Public Safety & Professional Communications Business Unit
Harris Corporation

Tania W. Hanna
Vice President, Legislative Affairs and Public Policy
Harris Corporation

Evan S. Morris, Esq.
Counsel, Government Relations
Harris Corporation

April 11, 2011